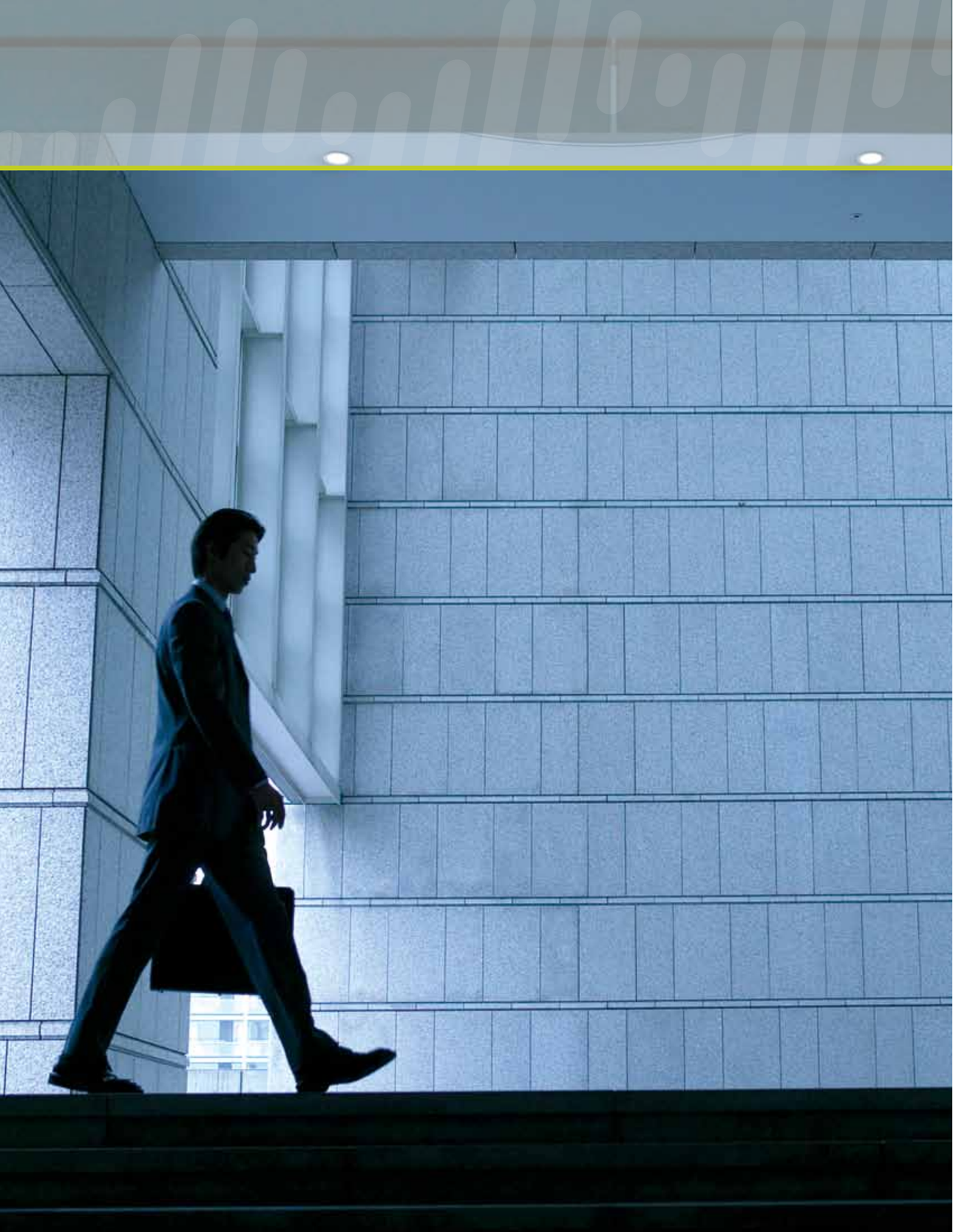
A Modern Framework for Network Security in the Federal Government

paloalto NETWORKS

the network security company™



Trends in Federal Requirements for Network Security

In recent years, federal agencies have seen a growing level of sophistication in the attacks levied against their networks. Intruders are exploiting blind spots in a network's defense, slipping past existing detection methods and blacklists. Attacks are leveraging the principles of stealth rather than force to gain entry. Some techniques trick well-meaning users into opening malicious websites or application-borne threats. Even the motivations for attacks are growing more diverse, ranging from hackers testing their skills against government systems, criminals looking for an exploitable opportunity, politically-driven opponents attempting to disrupt government services, and even foreign adversaries seeking intelligence.

A second challenge affecting network security strategies is striking the right balance between access to applications and preventing undesirable and illicit behavior. In the past, many organizations attempted to define proper use through limitations and restrictions, and a large list of exceptions. Such efforts proved to be difficult to manage and overly constrictive. In 2010, the U.S. Department of Defense took the prescient position that approved usage of Internet applications, including social media, on non-classified networks as long as proper controls are in place.[1] Instead of trying to define all the ways to block usage, the DoD approach empowers users with access to both official and personal applications while maintaining standards.

The challenge for today's federal security teams is develop a strategy that takes both the modern threat landscape and requirements for safe access into consideration. At times, it seems that every step towards one goal makes the other more difficult to achieve. It's becoming clear, however, that the limitations of existing network security technologies are part of the problem. What's needed is a plan that addresses today's goals without having to make compromises on either appropriate access or security.

Advanced Persistent Threats: *Advanced persistent threats (APT) and modern malware employ a number of techniques to enter and remain operational within a target organization. Some slip right past the traditional firewall and intrusion protection system, disguised or bundled within legitimate network traffic and application data.*

Once inside the trusted security domain, an APT can maintain communication channels with an attacker. It can exfiltrate intelligence and receive further instruction through an encrypted tunnel to an external command and control center. In addition, it can receive code updates which are reassembled within the compromised target to make signature detection more difficult and to add even more powerful and damaging capabilities.

Defining the Challenge: The Indiscriminate Network Perimeter

The firewall is the only place in the network that sees all network traffic passing across trusted and untrusted boundaries. However, legacy port-based firewalls assumed that each application and service communicates on a specific port. Today, such assumptions are no longer valid, because applications are sharing ports, hopping around on different ports, and some are intentionally using evasive techniques. A port-based policy is insufficient to determine which applications should be allowed network access.

In order to shore up the port-based firewall's application blindness, security organizations have been compensating by adding a long list of point products such as file scanning gateways, proxies, intrusion detection systems. Compliance directives such as the White House Comprehensive National Cybersecurity Initiative (CNCI) of 2009, made notable recommendations to add additional protections to stop malicious network behavior that makes it past the network edge:

Initiative #2: Deploy an intrusion detection system of sensors across the Federal Enterprise.

Initiative #3: Pursue deployment of intrusion prevention systems across the Federal Enterprise.

Such efforts are noble in intent, but the addition of even more systems to manage disparate policies creates greater administrative hardships upon agencies. The burden of adding more moving parts with different administrative tools and policies strains staffing requirements and increases the possibility of getting something wrong.

In the broader context, there are several notable issues at play:

1. There are many applications in use on every network, many of which are authorized, some of which are not.
2. Too much traffic is getting past the firewall. Without understanding the content, it is impossible to tell how much traffic contains unknown elements, where it's going, and whether it's for authorized or undesirable purposes.
3. The traditional port based firewall has a binary view of network traffic – either allow or deny, with almost no ability to make decisions based on the content. The port-based firewall can make a great fence, but has serious deficiencies with its guard post capabilities. It does not understand what's passing through.
4. Most network security point products do not have the ability to safely enable application usage. Most products are modeled on blocking usage rather than enablement.
5. Adding more products to an environment to address the deficiencies of the firewall has contributed to significant network complexity issues and higher operational cost.

Rather than making apologies for the firewall's deficiencies, perhaps it's time to ask what criteria the firewall should use to make decisions. Such questions should address policy in human recognized terms, such as:

- What applications are being used?
- Who is using the application?
- What information (or threat) is being sent to/from this application?

It's time to elevate expectations of what the firewall should do.

"Threats have gradually moved from being most prevalent in lower layers of network traffic to the application layer, which has reduced the general effectiveness of firewalls in stopping threats carried through network communications."

Guidelines on Firewalls and Firewall Policy
National Institute of Standards and Technology
NIST Special Publication 800-41 Revision 1, September 2009

Palo Alto Networks Solutions for Federal Government

The Palo Alto Networks™ next-generation firewall (NGFW) uses a different approach to security that follows a model of positive enforcement: Determine what applications, users and content that should be allowed, and enforce policy controls to restrict or block everything else.

The core technologies behind the next generation firewall:

App-ID™: Classify all traffic, on all ports, all the time—irrespective of protocol, encryption or evasive tactic.

User-ID™: Securely enable applications on your network based on users and groups—not just IP addresses.

Content-ID™: Real-time content scanning blocks threats, controls web surfing and limits data and file transfers.

Together, these technologies help agencies safely enable the use of applications within their network environment. App-ID identifies the application traffic, regardless of the port that it users, allowing the organization to write policy specifically around what should and shouldn't be allowed. User-ID allows security teams to map policy to specific groups and users. Content-ID provides inspection for threats such as intrusion and brute force attempts as well as downloads of executable files, viruses, application exploits, and modern malware. In addition, Content-ID can be used to detect the transfer of specific data within the network traffic and take corrective action.

The Palo Alto Networks next-generation firewall performs these tasks in a single pass inspection of network traffic, and controlled through a single policy definition, eliminating inefficiencies and mistakes that arise when depending upon multiple, disparate systems to perform a sequence of actions. Policy decisions are made with clear insight of the traffic elements, ensuring that the firewall is both effective at allowing approved traffic and stopping that which is not.

Palo Alto Networks is based in Santa Clara, California, and all product design and engineering is done in the United States. The PA-5000, PA-4000, PA-2000 Series and the PA-500 are manufactured in the United States. In addition, Palo Alto Networks owns intellectual property used in original design manufacturer products, which are manufactured in Trade Agreement Act (TAA) designated countries.

The Palo Alto Networks next-generation firewall meets many 3rd party validation requirements for products used in government agencies. It is Common Criteria EAL2 validated (with EAL4 testing underway). The cryptographic modules are FIPS 140-2 level 2 validated. In addition, Palo Alto Networks products are listed on the Department of Defense Unified Capabilities Approved Product List.

"A NGFW capability is an important element as enterprises move away from having dedicated IPS appliances at their perimeter and remote locations. Vendors in this quadrant lead the market in offering new safe-guarding features, providing expert capability, rather than treating the firewall as a commodity."

Magic Quadrant for Enterprise Network Firewalls
Gartner Group, December 2011

Recommendations for Strengthening Network Security within the Federal Government

Learn more about the Palo Alto Networks next-generation firewall by getting a demonstration. For agencies looking to take the next step, an evaluation can identify the traffic that you expect to see and pinpoint traffic that merits further investigation.

Deploying Palo Alto Networks next-generation firewall is a sensible measure to address emerging application threats and compliance mandates. It can be deployed as a stand-alone firewall or in conjunction with an existing firewall deployment. NIST 800-41 recommends using multiple layers to provide defense-in-depth.

The additional protections provided by the Palo Alto Networks next-generation firewall helps organizations dial in the amount of defense in depth they want. It reduces the attack surface by cutting out unwanted application traffic, thus reducing the workload on downstream systems. In addition, agencies can reduce their total cost of ownership by eliminating redundant security measures such as legacy IDS/IPS, proxies and web security products.

The Palo Alto Networks next-generation firewall is the right place to address application access and network threats. Get started today by contacting federal@paloaltonetworks.com.

Email: federal@paloaltonetworks.com
Phone: 866.320.4788 / 408.753.4000
Web: www.paloaltonetworks.com
Facebook: https://www.facebook.com/PaloAltoNetworks
Twitter: https://twitter.com/PaloAltoNtwks

Create defense-in-depth. *Defense-in-depth involves creating multiple layers of security. This allows risk to be better managed, because if one layer of defense becomes compromised, another layer is there to contain the attack. In the case of firewalls, defense-in-depth can be accomplished by using multiple firewalls throughout an organization, including at the perimeter, in front of sensitive internal departments, and on individual computers. For defense-in-depth to be truly effective, firewalls should be part of an overall security that also includes products such as antimalware and intrusion detection software.*[2]

[1] William J. Lynn III, Deputy Secretary of Defense, "Directive-Type Memorandum (DTM) 09-026 - Responsible and Effective Use of Internet-based Capabilities", February 25, 2010

[2] National Institute of Standards and Technology, Guidelines on Firewalls and Firewall Policy NIST Special Publication 800-41 Revision 1, September 2009

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

Copyright ©2012, Palo Alto Networks, Inc. All rights reserved. Palo Alto Networks, the Palo Alto Networks Logo, PAN-OS, App-ID and Panorama are trademarks of Palo Alto Networks, Inc. All specifications are subject to change without notice. Palo Alto Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Palo Alto Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. **PAN_BR_FED_030612**